

SECRET

USIB-D-1.5/24

Final USIB-Approved
18 July 1962

UNITED STATES INTELLIGENCE BOARD

Policy Statement Concerning Counterintelligence

and Security Responsibilities

SECRET

Excluded from automatic
downgrading and
declassification

USIB-D-1.5/24
Final USIB-Approved
18 July 1962

UNITED STATES INTELLIGENCE BOARD

Policy Statement

Concerning


Counterintelligence and Security

Responsibilities

1. On 18 July 1962 the United States Intelligence Board approved a Policy Statement on Counterintelligence and Security Responsibilities (Attachment 1) and the attached Guide re Practices and Procedures for Counterintelligence and Security of Overseas Personnel and Installations (Tabs A, B and C).

2. Intelligence Board members are requested to take such actions as may be required to implement this approved Policy, utilizing the provisions of the Guide as appropriate.

25X1A


JAMES S. LAY, JR.
Executive Secretary

Attachment

Attachment 1
USIB-D-1.5/24
Final USIB-Approved
18 July 1962

UNITED STATES INTELLIGENCE BOARD

Policy Statement Concerning Counterintelligence
and Security Responsibilities

In order for the USIB member departments and agencies to carry out effectively their responsibilities for the security of overseas personnel and installations and without intent to infringe upon such broader authority or responsibility as any may now have under law, Executive Order or NSC directive, the United States Intelligence Board is agreed:

- a. There must be as close coordination as possible at all levels among the security and counterintelligence components of those USIB departments and agencies having overseas responsibilities in order that the hostile threat may be adequately assessed and effective countermeasures taken.

SECRET

- b. Pertinent information concerning the efforts and capabilities of the opposition against U. S. personnel and installations overseas should be given as broad dissemination as possible among the counterintelligence and security components without unduly endangering methods and sources. There should be a continual exchange of such information at the national level and in the field. It is suggested that all departments and agencies concerned (1) sanitize useful materials which they produce, with a view to providing protection at the point of origin, and (2) ensure that the dissemination restrictions of the originating agency be observed.
- c. To ensure the availability of pertinent security and counterintelligence information to departments and agencies concerned, appropriate information developed concerning opposition efforts and capabilities should be submitted as soon as possible for inclusion in the central counterintelligence repositories in accordance with DCID 5/3.

- d. Wherever possible and appropriate, there should be meetings in the field of security and counter-intelligence representatives of those agencies which have responsibilities in areas of mutual concern and have established liaison.
 - e. USIB member departments and agencies with overseas responsibilities are requested to initiate a review as they deem appropriate of their existing programs, regulations, practices, and procedures concerning counterintelligence and personnel and physical security utilizing the attached guide of desirable practices and procedures in this review.
- It is suggested that revision of existing programs, regulations, practices and procedures be made wherever applicable and appropriate to ensure a more effective system for the protection of installations and personnel overseas.

Guide re Practices and Procedures:

TAB "A" - Counterintelligence
TAB "B" - Personnel Security Overseas
TAB "C" - Physical Security

SECRET

USIB-D-1.5/24
Final USIB-Approved
18 July 1962

UNITED STATES INTELLIGENCE BOARD

GUIDE

PRACTICES AND PROCEDURES

FOR

COUNTERINTELLIGENCE

AND

SECURITY OF OVERSEAS

PERSONNEL AND INSTALLATIONS

SECRET

TAB "A"

USIB-D-1.5/24
Final USIB-Approved
18 July 1962

COUNTERINTELLIGENCE

1. Counterintelligence and Security Policy Directives

U. S. Security and Counterintelligence personnel should be familiar with the executive and interdepartmental directives governing Security and Counterintelligence. Of key importance are EO No. 10450, EO No. 10501, NSCID No. 5, DCID Nos. 5/1, 5/2, and 5/3. A thorough grasp of these orders and directives and scrupulous adherence to their provisions are essential to the coordination of U. S. defenses overseas.

Similarly, each Security and Counterintelligence Officer should be familiar with this paper and with all regulations governing Security and Counterintelligence within his own department or agency.

2. Dissemination of Security and Counterintelligence Information Affecting U. S. Personnel and Installations Abroad

Counterintelligence and Security information directly relevant to the security of U. S. personnel, installations, classified equipment and documents, and operations outside the U. S. should be made available to

SECRET

appropriate Security Officers and the Counterintelligence components of other U. S. agencies as rapidly and fully as circumstances permit.

Especially important is information about hostile intelligence services, as well as national and international Communism. Within these categories are included current information on organizations engaged in hostile clandestine activity, all personnel within such organizations, functions, modus operandi, resources, strengths and weaknesses, and the like.

Modus operandi information should include known facts about the use of such techniques as provocation, penetration, subversion, blackmail, sexual or other entrapment. For security purposes, an intensive examination of the adversary in a specific area, such as a major city abroad, is just as important as a broader view of a service or Communist organization in toto. Information which becomes available to Security and Counterintelligence Officers abroad should be promptly reported to the departmental headquarters concerned and thence, as appropriate and in conformance with DCID 5/3, to the central counterintelligence records. Within departments and agencies the exchange of such information between counterintelligence and security elements should be as rapid and complete as need-to-know and the protection of methods and sources will permit.

- 2 -

SECRET

a. Lateral Field Dissemination of Counterintelligence and Security Information

Lateral field dissemination of counterintelligence is frequently desirable from the viewpoint of speed and efficiency; but before undertaking lateral distribution, Security and Counterintelligence Officers should ensure that it does not conflict with departmental regulations designed to preserve the security of sensitive items of counterintelligence through centralized control.

b. Headquarters and Field Coordination: Security and Counterintelligence

The terms of coordination of the U. S. clandestine counterintelligence activities abroad are prescribed by DCID 5/1, DCID 5/2, and DCID 5/3. The cooperation of U. S. security components should also be close to facilitate a rapid and profitable sharing of experience.

c. Meetings in Field

Security and counterintelligence personnel overseas within areas of mutual concern and who have established liaison, should meet periodically as

appropriate to exchange pertinent security and counterintelligence information and to discuss mutual problems. Periodic meetings of such representatives in the field will permit more effective counteractions to be taken in matters of mutual concern.

- d. Preparation and Dissemination of Security Area Studies of Hostile Service and CP Capabilities Prepared by Security Components.

To supplement counterintelligence studies of foreign services and of Communism abroad, security studies of hostile capabilities in specified foreign areas should be undertaken by U. S. headquarters and field security components.

Frequently, a single case or incident serves as an excellent example by which information concerning local hostile capabilities and techniques can be assessed, reported and disseminated.

3. Notifying Appropriate Officials of Counterintelligence and Security Operations

Senior and Command Officials should be advised in full of security operations being conducted within

- 4 -

SECRET

their areas of jurisdiction. They should also be advised of counterintelligence information in accordance with the provisions of DCID 5/1.

4. Responsibility of U. S. Employees to Report Information of Counterintelligence or Security Interest

Employees of the U. S. Government stationed overseas, regardless of assignment, should report through appropriate channels, information of counterintelligence or security interest; i. e., any information reaching them and concerning (1) foreign intelligence or security services engaged in activity directed against U. S. security, (2) national or international Communist organizations similarly engaged, and (3) specific violations or intended violations of U. S. laws or security directives by U. S. personnel. Governmental employees overseas should be adequately briefed by Security Officers concerning the appropriate laws, directives, policies, security responsibilities, etc. They may also be briefed by counterintelligence or security personnel, as appropriate, on hostile capabilities, personnel, etc. Such counterintelligence briefings however, should be conducted only on a

need-to-know basis. The informed cooperation of U. S. Government employees abroad will undoubtedly further U. S. security interests.

5. Security of Communication Activities

Maximum security support should be given to all forms of communicating and transmitting classified information including electrical means. Detailed studies should be conducted of current systems, including messengers, couriers, pouches, cables, and other forms of transmitting and communicating classified information to determine whether the security of such systems is adequate. The security of cryptographic systems of communication, however, is the responsibility of communications officials.

At present, certain systems of communicating and transmitting classified information among and between components of the various departments and agencies are not under the control of any particular department or agency. As a result, the responsibility for security protection of such systems has not been clearly assigned to any specific agency or department. Security Officers should be concerned with all means of communicating and transmitting classified information

both domestically and overseas to ensure that maximum security support is given to limit the possibility of compromise. Where appropriate, joint studies should be conducted by those agencies utilizing the same facilities.

6. Periodic Reviews of Counterintelligence and Security Operations

Periodic reviews should be conducted by each department and agency of its security operations and programs affecting personnel and installations overseas and a report thereof made to the head of the department or agency. This report should include recommendations as appropriate for improvement of security. There should be close observance of the applicable provisions of DCID 5/1 to ensure that counterintelligence operations are systematically reviewed and reported.

Periodic reviews within each department and agency of security operations and programs affecting personnel and installations overseas should be conducted to assess the effectiveness of security measures taken and to ensure that maximum efforts are being directed in those areas where the major threat exists. The review should include a statement of accomplishments, pending actions, and objectives for

the following year. Through such a review, plans of action to best cope with the threat can be made known to appropriate officials of each department to ensure that maximum support is given to such programs.

7. Assignment of Trained Security and Counterintelligence Personnel Overseas

Wherever possible, and particularly in areas where the hostile threat is especially effective or intense, specially trained security and counterintelligence personnel should be assigned to security and counterintelligence duties. Such personnel should be retained in these positions for extended periods whenever possible.

It is especially important that qualified and experienced counterintelligence and security personnel, who are thoroughly trained, be assigned who will recognize the hostile threat and who will take appropriate measures to counter the threat. This should ensure continuity and the effective implementation of counterintelligence and security programs.

8. Assignment of Research Analysts to Security Components

There should be experienced research analysts

within the security headquarters component of each department and agency to study on a continuing basis its cases involving penetrations, provocations, blackmail attempts and all such hostile efforts directed against personnel and installations.

A continual study of hostile activities directed against U. S. personnel and installations is necessary to augment our knowledge of hostile patterns of operations, including techniques and possible targets. Security research analysis will assist in identifying and assessing the threat and thereby ensure that timely security counter-measures are taken.

9. Establishment of Training Programs

To ensure that Counterintelligence and Security personnel are kept abreast of counterintelligence and security programs, techniques and methods of reporting, training programs and facilities should be established and maintained where practicable on a regular basis. It would be advantageous if those agencies and departments which have established training programs could offer their

training facilities to personnel of other agencies which may not have similar facilities. This should result in a more uniform implementation of security and counterintelligence programs.

25X1A

Approved For Release 2000/08/28 : CIA-RDP78-04007A000900110007-4

Next 15 Page(s) In Document Exempt

Approved For Release 2000/08/28 : CIA-RDP78-04007A000900110007-4